جامعة بيرزيت

BIRZEIT UNIVERSITY

Secure Software Development (SWEN7302)
Dr: Ahmad Alsadeh

Homework Assignment #3

By Hanan Namrouti(1165217)

1. What is penetration testing?

Whole-system testing for security flaws and bugs

2. Which of the following are benefits of penetration testing?

Results are often reproducible

Compositionality of security properties means tested components are secure even if others change

3. What does it mean to "be stealthy" during a penetration test?

Using encryption during tests to make the source of attacks impossible to determine

4. What is a web proxy?

A piece of software that intercepts and possibly modifies requests (and responses) between a web browser and web server

5. What is Nmap?

It is a scanner which works by injecting packets to a range of addresses, and inferring what hosts and services might be at those addresses, based on the responses

6. What is ethical hacking?

Hacking systems (e.g., during penetration testing) to expose vulnerabilities so they can be fixed, rather than exploited

7. Which of the following statements describe fuzz testing (aka fuzzing)?

It is concerned with finding known-bad behaviors, like crashes and hangs

8. Which of the following are true of whitebox fuzzing?

It takes into account the program's internals in some manner when deciding which inputs to choose

9. Which of the following are true of mutation-based fuzzing?

It generates each different input by modifying a prior input

10. Which of the following styles of fuzzer is more likely to explore paths covering every line of

Whitebox

11. Which of the following are functions of a network-based fuzzer?

- **Acting as a client (Network fuzzers may play any role in a network communication)**
- **Acting as a "man in the middle (Network fuzzers may play any role in a network communication, and may intercept messages between legitimate roles)**

12. Suppose you want to use fuzzing on a program to try to find memory errors; which of the following statements are true?

Compiling the program with addresssanitizer (ASAN) will make the source of a memory error easier to find